УДК 343.713

СОДЕРЖАНИЕ И УГОЛОВНО-ПРАВОВАЯ ОЦЕНКА УГРОЗЫ УНИЧТОЖЕНИЯ, ЗАВЛАДЕНИЯ, БЛОКИРОВАНИЯ, МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ КИБЕРВЫМОГАТЕЛЬСТВЕ

Л. А. Рябцева
кандидат педагогических наук,
доцент кафедры общеюридических и уголовно-правовых дисциплин
факультета повышения квалификации и переподготовки кадров
Могилевского института МВД (Беларусь)

Увеличение количества кибервымогательств диктует необходимость поиска решения проблемы как на законодательном уровне, так и в разрезе правоприменительной практики. Многообразие выявленных способов, отличающих вымогательство, совершенное с использованием информационно-коммуникационных технологий, от его традиционных форм, актуализирует целесообразность пересмотра содержания угроз, сопровождающих данное преступление, в особенности тех, которые связаны с намерением виновного лица причинить существенный вред не только отношениям собственности, но и компьютерной безопасности. В настоящей связи автор, опираясь на нормативные правовые источники (Уголовный кодекс Республики Беларусь, Закон Республики Беларусь «Об информации, информатизации и защите информации»), судебные и доктринальные толкования, предпринимает попытку переосмысления содержания угрозы уничтожения, завладения, блокирования, модификации компьютерной информации, некоторых ситуативных особенностей ее реализации и правовой оценки.

Ключевые слова: *кибервымогательство; вымогательство; компьютерная информация; компьютерная безопасность; угроза уничтожения, завладения, блокирования; модификации компьютерной информации.*

Введение. Информатизация всех сфер жизни человека — современная тенденция, детерминируемая стремительно меняющимся мироустройством. Однако качественное преобразование ведущих направлений жизнедеятельности общества граничит с потенциальной угрозой компьютерной безопасности, которая может выступать непосредственным объектом (основным или дополнительным) противоправных посягательств. Риски причинения ей существенного вреда возрастают при совершении киберпреступлений, предполагающих не только само осуществление противоправных манипуляций с компьютерными данными (составы, предусмотренные гл. 31 Уголовного кодекса Республики Беларусь (далее — УК Республики Беларусь) «Преступления против компьютерной безопасности»), но и использование компьютерной системы (компьютера и подключаемого к нему оборудования) как инструмента совершения посягательств (например, для высказывания (передачи) угроз в отношении жизни, здоровья лица, его права собственности, чести и достоинства и др.) (составы, предусмотренные иными главами Особенной части УК Республики Беларусь) [1]. Общество и государство учатся справляться с подобными угрозами. Однако такой опыт не всегда является успешным.

Так, на фоне общего, хотя и незначительного (на 6 %), снижения в 2025 г. роста киберпреступлений по Республике Беларусь [2] регистрируется увеличение числа случаев кибервымогательства (+284 (41,6 %) в сравнении с 2024 г. [3, с. 2]), при совершении которого существенный вред, учитывая многообъектность преступления, причиняется или может быть причинен не только отношениям собственности, но и параллельно здоровью, чести и достоинству, деловой репутации, компьютерной безопасности потерпевших лиц.

Вместе с тем уголовно-правовое содержание отдельных угроз, высказанных при кибервымогательстве, а также последующая правовая оценка содеянного вызывают некоторые сложности. Актуальны случаи, когда угроза совершения перечисленных в диспозиции ч. 1 ст. 208 УК Республики Беларусь действий в части, касающейся завладения, блокирования, модификации компьютерной информации, фактически отсутствует (не высказывается потерпевшему), а требование о передаче имущества, права на имущество либо совершения каких-либо действий имущественного характера выдвигается как условие ее возврата собственнику или владельцу в неизменном виде или возвращения последнему доступа к ней. С учетом этого возникает противоречие между содержанием уголовно-правовой нормы, предусматривающей ответственность за вымогательство с обозначенным видом угрозы (ст. 208 УК Республики Беларусь), и отсутствием подходов в юридической оценке случаев, когда субъект преступления обещает вернуть или разблокировать компьютерную информацию под предлогом ее выкупа.

Несмотря на то, что изучению сущности кибервымогательства и отдельных ее аспектов посвящены работы российских (Т. М. Лопатина [4], Л. Д. Матросова [5], А. Д. Чурсина [6], И. Д. Прудников [7], М. М. Моргунова [8] и др.) и белорусских исследователей (О. И. Бахур [9], О. О. Топорикова [10] и др.), проблема сохраняет свою актуальность, поскольку содержание российских исследований не в полной мере коррелирует с белорусским уголовным законодательством, а среди работ отечественных ученых единственный вариант уголовно-правовой оценки был предложен О. И. Бахуром.

В настоящей связи была определена цель исследования — выработать обоснованную позицию относительно решения проблемы, связанной с уголовно-правовой оценкой требования передачи имущества, права на имущество или совершения действий имущественного характера, следующего за состоявшимся фактом завладения, блокирования или модификации компьютерной информации. Поставленная цель была достигнута путем решения следующих задач: проанализировать с опорой на существующие источники современное содержание угрозы уничтожения, завладения, блокирования, модификации компьютерной информации при кибервымогательстве, оценить обоснованность признания вымогательством случаев требования выкупа за ее разблокировку.

Основная часть. Обозначенная ситуация является предметом обсуждения как на уровне уголовно-правовой доктрины, так и на уровне правоприменительной практики, что подтверждается действующими положениями разработанного Комплексного плана мероприятий, направленных на принятие мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2026–2027 годы, в том числе в части, касающейся анализа применения уголовного законодательства (п. 19) [11] с целью его последующего возможного совершенствования. Особую актуальность реализация указанного плана приобретает на фоне роста случаев кибервымогательства, способы совершения которого системно представлены главным управлением по противодействию киберпреступности криминальной милиции Министерства внутренних дел Республики Беларусь [3]. Их анализ позволяет установить, что среди наиболее распространенных случаев кибервымогательства выделяются виды, связанные: 1) с блокированием, модификацией или уничтожением компьютерной информации; 2) с угрозой распространения личной информации потерпевших либо иных сведений, которые они желали сохранить в тайне; 3) с угрозой применения насилия. Из четырех альтернативных угроз, обозначенных в ч. 1 ст. 208 УК Республики Беларусь, любая из которых должна сопровождать требование передачи имущества, права на имущество либо совершения действий имущественного характера, только угроза уничтожением или повреждением имущества потерпевших лиц не так часто встречается при совершении вымогательства с использованием информационно-коммуникационных

технологий [1; 3]. Это значит, что указанные в диспозиции ч. 1 ст. 208 УК Республики Беларусь угрозы приобрели новые формы выражения, отвечающие процессам цифровизации общества.

Сравнительный анализ способов реализации угроз, присущих вымогательству, совершаемому без использования информационно-коммуникационных технологий, и способов их выражения при кибервымогательстве позволяет заключить, что частым поводом высказываемых в последнем случае угроз выступает предшествующая активность лица в интернет-пространстве, связанная с желанием устроить личную жизнь (посещение сайтов знакомств или общение в социальной сети с такой целью), получить сексуальные услуги (посещение интернет-ресурсов, предлагающих интимные услуги), трудоустроиться и др. [3, с. 3]. В таких случаях предметом преступного посягательства становится компьютерная информация, в большинстве своем добровольно предоставленная злоумышленнику потерпевшим (например, фото-, видеоизображения, личные данные и др.).

Сама по себе *угроза уничтожения, завладения, блокирования, модификации компьютерной информации* предполагает, что специфическим дополнительным предметом преступления, помимо тех трех, что заявлены в диспозиции ст. 208 УК Республики Беларусь, является компьютерная информация.

В ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» информация определена как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». В ст. 28 названного Закона прямо указано, что «защите подлежит информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу» [12].

Понятием компьютерной информации охватывается программное обеспечение, а также «сведения, представляющие ценность для государства, общества и отдельных граждан, хранение, использование и производство различных операций с которыми осуществляется посредством компьютерной техники» [13, с. 771].

Для состава кибервымогательства оба значения понятия компьютерной информации являются вполне допустимыми. Однако содержание угрозы, альтернативно предполагающей, согласно диспозиции ч. 1 ст. 208 УК Республики Беларусь, уничтожение, завладение, блокирование или модификацию компьютерной информации, в некоторых случаях сложно соотнести с реально высказываемой угрозой. В этой связи необходимо четко понимать смысл каждого из заявленных общественно опасных действий, способных составить содержание угрозы, подкрепляющей требование о передаче имущества, права на имущество и совершении действий имущественного характера, что представляется затруднительным при отсутствии официального толкования.

Согласно «Толковому словарю современного русского языка» Д. Н. Ушакова, уничтожить означает «истребить, разрушить, прекратить существование… чего-нибудь» [14, с. 708], завладеть — «взять себе… что-нибудь, захватить» [14, с. 146]. В то же время «блокирование» образовано от «блокировать», то есть «прекратить (прекращать) доступ куда-либо… работу какого-либо механизма; воспрепятствовать (препятствовать) осуществлению чего-либо, уменьшить (уменьшать) активность, парализовать чью-либо деятельность» [15, с. 349]. Понятие модификации компьютерной информации предусмотрено непосредственно в примечании к ст. 208 УК Республики Беларусь и подразумевает ее противоправное изменение либо «внесение в компьютерную систему заведомо ложной компьютерной информации» [1].

То есть по смыслу приведенных выше понятий угроза уничтожить компьютерные данные потерпевшего является намерением физически их ликвидировать (полностью или значительную часть) без возможности последующего восстановления. При кибервымогательстве подобного рода угроза может выражаться, например, в высказывании намерения удалить электронный документ, принадлежащий

потерпевшему (дипломная работа, диссертация, авторское произведение и др.), размещенный в облачном хранилище. В случае ее реализации файл прекратит свое физическое существование.

Угроза завладением компьютерной информацией предполагает ее захват, противоправное изъятие из собственности, владения потерпевшего с одновременным обращением в обладание виновного. Важно, чтобы похищаемые данные представляли для потерпевшего ценность, были значимыми.

Угроза блокированием компьютерной информации включает в себя выраженное намерение совершить действия, результатом которых станет полная (отказ в доступе к данным) или частичная (открывать, копировать, переименовывать и др.) невозможность потерпевшего работать с данными.

Под угрозу модификации компьютерной информации путем ее изменения, представляется, попадают случаи ее искажения, например, путем использования вредоносных программных продуктов для шифрования файлов [3, с. 7].

Вымогательство, в том числе кибервымогательство, какой бы вид угрозы, заявленный в диспозиции ч. 1 ст. 208 УК Республики Беларусь, ни использовал субъект, имеет формальный состав и будет считаться юридически оконченным с момента высказывания требования, подкрепленного угрозой, независимо от того, будет ли последняя исполнена [16]. Вместе с тем содержанием квалифицирующих признаков вымогательства предусмотрена фактическая реализация отдельных из угроз посредством указания на факт их исполнения: применение как не опасного (ч. 2 ст. 208 УК Республики Беларусь), так и опасного для жизни и здоровья насилия (ч. 3 ст. 208 УК Республики Беларусь), уничтожение или повреждение имущества (ч. 2 ст. 208 УК Республики Беларусь). Приведенные в исполнение угрозы становятся средством давления, обеспечивающим гарантированное, с точки зрения субъекта преступления, беспрецедентное выполнение потерпевшим его требований. Однако, согласно содержанию ст. 208 УК Республики Беларусь, требование в отношении одного из предметов преступления обязательно высказывается параллельно (одновременно) с угрозой или при наличии крайне незначительного разрыва во времени между ними [1]. Логическая последовательность актов преступного поведения сохраняется: требование предшествует угрозе или фактическому ее исполнению.

Вместе с тем применительно к анализируемой угрозе уничтожения, завладения, блокирования, модификации компьютерной информации, высказываемой в связи с кибервымогательством, на практике преобладают ситуации, когда лицо изначально совершает определенные действия, результатом которых становится исключение физической возможности потерпевшего управлять информацией (в том числе путем блокирования его аккаунта), а после выдвигает ему требование передачи имущества (чаще всего) за возврат доступа к учетной записи пользователя. Такого рода посягательства в большинстве своем фиксируются в отношении владельцев мобильных устройств Apple [3].

Закономерно возникает вопрос, насколько подобные действия лица, имеющего корыстную цель, охватываются составом вымогательства. Ситуация, при которой мы сталкиваемся не с выраженным намерением лица уничтожить, завладеть, блокировать, модифицировать компьютерную информацию, сопровождающим требование передачи имущества, права на имущество или совершения действий имущественного характера, а со случившимся фактом совершения одного или нескольких действий, входящих в состав описанной угрозы, не подпадает под признаки вымогательства, так как виновный на момент высказывания требования к потерпевшему лицу никаких угроз не выражает, поскольку акт преступного поведения, заложенного в содержание обозначенной угрозы, уже состоялся.

Обратившись к законодательному и правоприменительному опыту Российской Федерации, можем констатировать следующее. Некоторые исследователи (Т. М. Лопатина, И. Д. Прудников и др.) высказывают мнение о том, что получение

выкупа за разблокировку аккаунта, доступ к компьютерной информации, охватывается составом вымогательства [4; 7]. Парадоксально, что подобный подход существует в условиях, когда в диспозиции ст. 163 Уголовного кодекса Российской Федерации «Вымогательство» отсутствует угроза совершения противоправных действий в отношении компьютерной информации [17]. И. Д. Прудников, обращая на это внимание, предлагает дополнить объективную сторону вымогательства еще одной угрозой «в виде блокирования, копирования или уничтожения компьютерной информации либо условия для прекращения блокирования, копирования или уничтожения компьютерной информации» [7, с. 433], которая частично представлена в ст. 208 УК Республики Беларусь.

А. А. Гребеньков подчеркивает, что кибервымогательство обладает признаками как преступлений против компьютерной безопасности, так и преступлений против собственности (использует понятие «классическое вымогательство»), но ни к одной из двух групп в полной мере не относится. В настоящей связи автор указывает на необходимость разработки специальной уголовно-правовой нормы, регламентирующей ответственность за кибервымогательство [18, с. 153].

Среди белорусских ученых попытка правовой оценки состоявшегося завладения, блокирования мобильных устройств, учетной записи (аккаунта) или иной компьютерной информации потерпевшего для получения от него денежных средств за возвращение доступа к ним предпринята О. И. Бахуром. Исследователь считает квалификацию содеянного по признакам вымогательства необоснованной, мотивируя тем, что, во-первых, в диспозиции ч. 1 ст. 208 УК Республики Беларусь представлен исчерпывающий перечень угроз, во-вторых, любая угроза есть всего лишь намерение осуществить противоправное воздействие, а завладение или блокирование — состоявшийся акт преступного поведения, требующий самостоятельной правовой оценки (как преступление против компьютерной безопасности) [9, с. 92]. В этой части с ним можно согласиться. Вместе с тем предложенная автором квалификация по совокупности преступлений (ст. 349, 350, 185 УК Республики Беларусь) требует некоторого осмысления, в том числе и в связи с бланкетным характером диспозиций преступлений против компьютерной безопасности. Так, ряд признаков объективной стороны данных составов может быть правильно истолкован только с опорой на содержание Закона Республики Беларусь «Об информации, информатизации и защите информации» (доступ к информации, система защиты, виды мер по защите информации и их содержание).

Помимо этого, применение ч. 1 ст. 349 УК Республики Беларусь («Несанкционированный доступ к компьютерной информации») для формального состава преступного поведения требует наличия мотива в виде корыстной заинтересованности. В то же время обязательным условием наступления уголовной ответственности по ч. 1 ст. 350 УК Республики Беларусь «Уничтожение, блокирование или модификация компьютерной информации» является одновременное отсутствие признаков преступления против собственности и наличие общественно опасного последствия в виде существенного вреда, характеризующегося оценочностью его установления. Объективная сторона принуждения (ст. 185 УК Республики Беларусь) предполагает психическое воздействие на потерпевшего, при котором виновный желает добиться от последнего определенной линии поведения. В данном случае мотив не имеет уголовно-правового значения и может быть любым, в том числе и корыстным.

Заключение. Как видим, такая квалификация действий лица, требующего выкуп под условием разблокировки компьютерной информации, принадлежащей потерпевшему, не позволяет признать правовую оценку содеянного понятной и очевидной процедурой, а даже, наоборот, обременяет процесс правоприменения, что указывает на необходимость поиска решения проблемы путем возможного внесения изменений в ст. 208 УК Республики Беларусь в части, касающейся факта реализованной

угрозы противоправных действий с компьютерной информацией, либо дополнения существующего постановления Пленума Верховного Суда Республики Беларусь «О применении судами уголовного законодательства по делам о хищениях имущества» [16] положением, предусматривающим особенности квалификации подобного преступного поведения в системе официального толкования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 20 окт. 2025 г. № 101-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 25.03.2026).
2. МВД: в 2025 году количество киберпреступлений в Беларуси сократилось на 6 % // SB.BY. Беларусь сегодня. – URL: https://www.sb.by/articles/kolichestvo-kiberprestupleniy-v-2025-godu-snizilos-na-6-mvd.html. – Дата публ.: 03.02.2026.
3. Конспект с актуальными способами совершения кибервымогательств / М-во внутр. дел Респ. Беларусь ; Кримин. милиция ; Гл. упр. по противодействию киберпреступности ; сост. П. С. Ленский. – Мн. : [б. и.], 2026. – 13 с.
4. Лопатина, Т. М. Условно-цифровое вымогательство, или кибершантаж / Т. М. Лопатина // Журнал российского права. – 2015. – № 1 (217). – С. 118–126.
5. Матросова, Л. Д. Системный анализ понятия средств реализации и принятия решений по совершенствованию мер защиты от вымогательства в сети Интернет / Л. Д. Матросова // Закон и право. – 2018. – № 11. – С. 152–154.
6. Чурсина, А. Д. Кибервымогательство и угрозы в социальных сетях / А. Д. Чурсина // Вестник Московского университета МВД России. – 2022. – № 5. – С. 294–296.
7. Прудников, И. Д. Уголовно-правовая оценка кибервымогательства / И. Д. Прудников // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия: Гуманитарные науки. – 2023. – Т. 17, № 3 (65). – С. 426–433.
8. Могунова, М. М. Уголовно-правовой анализ киберугроз в деловой среде / М. М. Могунова // Вестник Омского университета. Серия: Право. – 2021. – Т. 18, № 1. – С. 89–95.
9. Бахур, О. И. Уголовная ответственность за кибервымогательство по уголовному законодательству Республики Беларусь / О. И. Бахур // Уголовная политика и культура противодействия преступности : материалы Междунар. науч.-практ. конф. памяти проф. В. Е. Квашиса, г. Краснодар, 20 сент. 2024 г. / Краснодар. ун-т МВД России ; редкол.: А. Л. Осипенко [и др.]. – Краснодар, 2024. – С. 88–92.
10. Топорикова, О. О. Сексуальное кибервымогательство / О. О. Топорикова // Теоретические и прикладные проблемы информационной безопасности : материалы Междунар. науч.-практ. конф., г. Минск, 18 мая 2017 г. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич [и др.]. – Мн., 2018. – С. 67–70.
11. Комплексный план мероприятий, направленных на принятие мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2026–2027 годы // Центральная система государственных публичных библиотек г. Могилева. – URL: https://csgpb.by/biblioteka/wp-content/uploads/2026/02/kompleksnyj-plan-na-2026-2027-gg.pdf (дата обращения: 25.03.2026).
12. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З : в ред. от 10 окт. 2022 г. № 209-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 26.03.2026).
13. Уголовный кодекс Республики Беларусь: научно-практический комментарий / Т. П. Афонченко, Н. А. Бабий, Н. А. Швед [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. – Мн. : Нац. центр правовой информ. Респ. Беларусь, 2019. – 1000 с.
14. Ушаков, Д. Н. Толковый словарь современного русского языка / Д. Н. Ушаков. – М. : Аделант, 2014. – 800 с.
15. Академический толковый словарь русского языка. – М. : Языки славянской культуры, 2016. – Т. 1 : А — ВИЛЯТЬ / авт.-сост. Л. П. Крысин, А. С. Кулева, И. В. Нечаева, Л. Л. Шестакова [и др.]. – 671 с.
16. О применении судами уголовного законодательства по делам о хищениях имущества : постановление Пленума Верхов. Суда Респ. Беларусь от 21 дек. 2001 г. № 15 : в ред. от 30 сент. 2021 г. № 8 // ЭТАЛОН : информ.-поисковая система (дата обращения: 26.03.2026).

17. Уголовный кодекс Российской Федерации : 13 июня 1996 г. № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. от 9 апр. 2026 г. № 100-ФЗ // КонсультантПлюс. Россия : справ. правовая система (дата обращения: 12.04.2026).

18. Гребеньков, А. А. Кибервымогательство как информационное преступление / А. А. Гребеньков // Экономика, управление и право: инновационное решение проблем : сб. ст. IX Междунар. науч.-практ. конф., г. Пенза, 25 авг. 2017 г. / под общ. ред. Г. Ю. Гуляева. – Пенза : Наука и Просвещение, 2017. – С. 152–154.

Поступила в редакцию 10.04.2026 г.
Контакты: hpkf1983@mail.ru (Рябцева Людмила Александровна)

Rabtsava L. A.

CONTENT AND CRIMINAL LAW ASSESSMENT OF THE THREAT OF DESTRUCTION, SEIZURE, BLOCKING, AND MODIFICATION OF COMPUTER INFORMATION DURING CYBER EXTORTION

The rise in cyber extortion necessitates finding solutions both at the legislative level and through law enforcement. The diversity of identified methods that distinguish extortion committed using information and communication technologies from its traditional forms highlights the need to review the content of the threats accompanying this crime, particularly those linked to the perpetrator's intent to cause significant harm not only to property relations but also to computer security. In this regard, the author, relying on normative legal sources (the Criminal Code of the Republic of Belarus, the Law of the Republic of Belarus «On Information, Informatization and Protection of Information»), judicial and doctrinal interpretations, attempts to rethink the content of the threat of destruction, seizure, blocking, and modification of computer information, some situational features of its implementation and legal assessment.

Keywords: *cyber extortion; extortion; computer information; computer security; threat of destruction, seizure, blocking; modification of computer information.*